PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-069549**
(43)Date of publication of application : **07.03.2003**

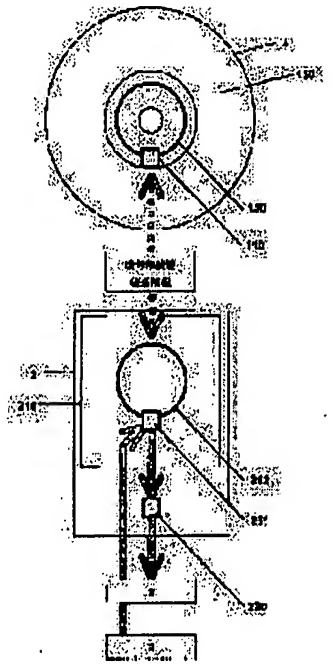
(51)Int.Cl. **H04L 9/08**
G06K 19/07
G06K 19/073
G09C 1/00
H04L 9/10

(21)Application number : **2001-252487**
(22)Date of filing : **23.08.2001**

(71)Applicant : **HIRANO DESIGN SEKKEI:KK**
(72)Inventor : **HIRANO TETSUYUKI**
OKI MASABUMI

(54) INFORMATION PROTECTION MANAGEMENT SYSTEM USING RFID MOUNTED STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system, which provides encrypted information by a recording medium and safely provides a decrypting key for decrypting the information.
SOLUTION: In an information providing system using a RFID (radio frequency identification) mounted storage medium, in which encrypted information is recorded and a RFID chip is appended to, the invention is an information protection management system using a RFID mounted storage medium that is characterized in that the system comprises (1) a means for distributing a decrypting key from an information supplier and for recording it in a RFID chip of user's RFID mounted storage medium, and (2) a means for reading the decrypting key from the RFID chip and for decrypting encrypted information by the decrypting key for usage when encrypted information is read from the RFID mounted storage medium.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－69549
（P2003－69549A）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04L 9/08		G09C 1/00	660D	5B035
G06K 19/07		H04L 9/00	601B	5J104
19/073			621A	
G09C 1/00	660	G06K 19/00	P	
H04L 9/10			H	

審査請求　未請求　請求項の数6　ＯＬ　（全８頁）

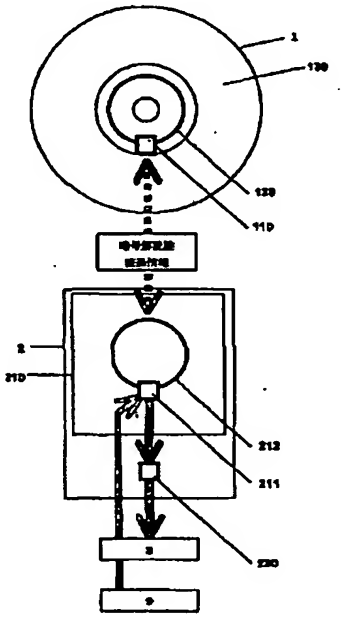
(21)出願番号　特願2001－252487(P2001－252487)
(22)出願日　平成13年８月23日(2001.8.23)

(71)出願人　592260343
株式会社平野デザイン設計
東京都世田谷区深沢８丁目12番７号
(72)発明者　平野　哲行
東京都世田谷区深沢８丁目12番７号　株式会社平野デザイン設計内
(72)発明者　大木　正文
東京都世田谷区深沢８丁目12番７号　株式会社平野デザイン設計内
(74)代理人　100093517
弁理士　豊田　正雄

最終頁に続く

(54)【発明の名称】　ＲＦＩＤ搭載記録媒体利用の情報保護管理システム

(57)【要約】
【課題】　暗号化された情報（暗号化情報）を記録媒体で提供し、解読するための復号化鍵を安全に提供するシステム。
【解決手段】　暗号化された情報が記録された記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)情報提供者から復号化鍵を配信してユーザーのRFID搭載記録媒体のRFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記復号化鍵を読み取り、該復号化鍵で前記暗号化された情報を復号化して利用する手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システムとする。



1

【特許請求の範囲】

【請求項１】暗号化された情報が記録された記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)情報提供者から復号化鍵を配信してユーザーのRFID搭載記録媒体のRFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記復号化鍵を読み取り、該復号化鍵で前記暗号化された情報を復号化して利用する手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システム。

【請求項２】記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)暗号化された情報と復号鍵をサーバーより配信し、前記暗号化された情報は前記記録媒体に、復号鍵は前記RFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記復号化鍵を読み取り、該復号化鍵で前記暗号化された情報を復号化して利用する手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システム。

【請求項３】記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)暗号化された情報と復号鍵をサーバーより配信し、前記暗号化された情報と前記復号鍵は前記記録媒体に、前記復号鍵に対応したIDを前記RFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記IDを読み取り、前記記録媒体から読み出した復号鍵と比較し、前記IDに対応する復号化鍵である場合は前記暗号化された情報を復号化して利用し、前記IDに対応しない復号化鍵の場合は前記暗号化された情報を復号化しない手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システム。

【請求項４】前記配信がインターネットを用いるものであることを特徴とする請求項１乃至３記載のRFID搭載記録媒体利用の情報保護管理システム。

【請求項５】前記配信が専用線を用いるものであることを特徴とする請求項１乃至３記載のRFID搭載記録媒体利用の情報保護管理システム。

【請求項６】前記配信が無線を用いるものであることを特徴とする請求項１乃至３記載のRFID搭載記録媒体利用の情報保護管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、大容量記録媒体で情報を提供する場合、記録媒体に暗号化されて記録されている情報を利用できるように復号化鍵をインターネットで配信する手段を有し、かつ、当該記録媒体に対する、コピーによる情報の不正使用防止を目的とした情報保護管理システムに関する。

【０００２】

2

【従来の技術】現在、情報の多くは電子情報として記録媒体に記録・保存されている。また情報の提供も、記録媒体で行われている。電子情報はコピーしやすく、加工しやすいなどの利点がある。通信で送信することもでき、またコピーして多数のユーザーに送信することも容易である。この便利な特徴ゆえに、記録情報のコピーによる不正使用や盗用による不正利用が社会問題となっている。

【０００３】例えば、CDやDVDなどで提供されている音楽、映画、プログラム、商用統計データなどの情報（データ）が他の記録媒体にコピーされ、不正に使用されている。このような不正利用を防止するために、一般に情報を暗号化して記録媒体に記録して提供する方法がとられている。この場合、CDやDVDなどの記録媒体に登録された情報を利用するときには、情報の提供源から復号化鍵（暗号解読鍵）を入手する必要がある。暗号化情報が記録された記録媒体は通信販売や店で入手し、復号化鍵はインターネットで入手する形態もある。最近の記録媒体は大容量であるために、複数種類の情報が１枚の記録媒体に登録されている。情報はそれぞれ異なる暗号化鍵で暗号化されていて、利用したい情報に対してはその情報に対する復号化鍵を購入する形態がとられている。

【０００４】インターネットで情報を提供する方法も最近はごく普通に行われている。情報が生のデータで送信される形態もまだ多いが、暗号化による方法も広く採用されるようになってきている。例えば、暗号化情報をまず送り、その後で復号化鍵を送信する方法がある。その多くは、復号化鍵をメールで送り、ユーザーが復号化鍵を入力することによって、暗号化情報を復号化して利用する形態である。この場合、暗号化情報がコピーされたとき、復号化鍵が第三者に漏れ、コピー情報が不正に使用される危険性がある。また、同じ記録媒体に復号化鍵を自動的に書き込む方法もあるが、媒体内の鍵も同時にコピーできるために、不正使用を防ぐことはできない。

【０００５】個人認証、商品の識別、位置測定などのツールとして最近、RFIDが注目されている。RFID（Radio Frequency IDentification：無線周波による非接触自動識別技術）には情報が蓄えられ、非接触による読み取りが可能な技術である。例えば、高速料金所での自動車の自動識別にRFIDが用いられ、自動判別に従って高速料金を自動徴収するという高速料金徴収システムである。この方法では、自動車に搭載したRFIDチップに個人情報が記録されていて、料金所に据え付けのRFIDリーダーによって非接触でRFIDの情報が読み取られ、読み取られた個人情報は中央のコンピュータに送られ、課金が行われる。

【０００６】RFIDチップは非接触で記録情報が読み取れ、無電池で動作し、耐久性、耐候性に優れている。RFIDチップは無電池であるが、RFIDリーダー／ライターから発せられる電波による電磁誘導よってRFIDチップ内に

電流が流れ、RFIDチップ内に組み込まれた回路が作動する仕組みになっている。RFIDチップにコンピュータ回路を組み込むこともでき、情報の記録保存の道具としてだけでなく、セキュリティ管理などの論理回路も組み込める。またRFIDチップには不揮発性のRAM（読み書きが可能で、メモリ内の記録がバッテリなしに保存されるタイプのメモリ）が用いられ、通常はROM的な利用方法がとられている。例えば定期券にRFIDチップを埋め込み、非接触型で自動改札処理を行う利用形態や、身分証明証にRFIDチップを埋め込んで個人認証を行う利用形態などが考えられている。RFIDチップの大きさやそれにつなげるアンテナの長さによって、コンマ数ミリメーターの距離から数メーターの距離まで、非接触動作ができる。このため、幅広い分野での応用が期待されている。

【０００７】RFIDに関する特許出願も多く、『非接触データ・キャリア・システムにおける不正アクセス防止方法』（特開2000-259571）や『商品管理』（特開2001-031218）などがある。前者はRFIDコンピュータへの不正アクセスを防止する方法であり、後者はRFIDチップを商品に貼り付けて商品の管理を行う管理方法である。

【０００８】

【発明が解決しようとする課題】情報のデジタル化の発展には目を見張るものがあり、かつてのようにコード情報（テキスト情報）だけでなく、画像データや音声データなどの大容量データの取り扱いもごく日常的なものとなっている。すべてのテレビ放送がデジタル放送に切り換わる日も、そう遠い未来ではないであろう。デジタル情報の利点はコピーが容易なこと、コピーによる劣化がないこと、加工がしやすいことなどが挙げられる。アナログデータはコピーによりデータが劣化し、何度かコピーを重ねると元の情報が変形してしまう。これに対してデジタル情報は何度コピーしても劣化が起こらず、コピーによって不正に利用されるなどの問題点もある。

【０００９】ブロードバンド（高速・大容量）が進むなか、インターネットによる音楽や映像の配信が注目を浴びている。音楽や映像はデジタル化されているために、コンピュータ処理が容易であり、配信やコピーによるデータ劣化がないのもデジタル情報の強みである。またデータ圧縮も可能であり、大量データをネットで扱う点においても、アナログデータに比べて有利である。その反面、不正情報配信やコピーによる不正利用が社会的な問題となっている。その一つに、ナップスター問題がある。許可を得ていない情報がインターネット上で不正に交換されるために、権利所有者側と著作権問題で争いになっている。

【００１０】複数の情報を暗号化して１枚の大容量記録媒体に記録し、店頭や通信販売で提供する新たな情報提供形態も盛んになってきている。媒体に記録された情報（音楽、映画、ゲーム等）はサンプルラン（いわゆる試聴、試写など）が行え、ユーザーはそのサンプルランによってどの情報を買うかを決められるなどの利点がある。ユーザーが情報を購入する場合、購入した店で復号化鍵を購入するか、インターネットで復号化鍵を送信してもらう方法がとられている。以前はユーザーがメールなどで送られてくる復号化鍵を直接入力する方法がとられていたが、最近は情報配信システムが直接記録媒体に書き込む方法に切り換わっている。要するに、復号化鍵をユーザーに知られることを避けるためである。しかし情報と同じ記録媒体に書き込まれているために、情報と復号化鍵が同時にコピーされることから、コピーによる不正利用に対して完全とは言えない。

【００１１】本発明が解決しようとする課題は、暗号化された情報（暗号化情報）を記録媒体で提供し、解読するための復号化鍵を安全に提供するシステムを提唱することにある。また本発明では、インターネットによる暗号化情報およびその復号化鍵を安全に提供することも目的とする。

【００１２】

【課題を解決するための手段】上記課題を解決するために、請求項１に記載された発明は、暗号化された情報が記録された記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)情報提供者から復号化鍵を配信してユーザーのRFID搭載記録媒体のRFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記復号化鍵を読み取り、該復号化鍵で前記暗号化された情報を復号化して利用する手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システムとする。

【００１３】請求項２に記載されたシステムは、記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)暗号化された情報と復号鍵をサーバーより配信し、前記暗号化された情報は前記記録媒体に、復号鍵は前記RFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記復号化鍵を読み取り、該復号化鍵で前記暗号化された情報を復号化して利用する手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システムとする。

【００１４】請求項３に記載されたシステムは、記録媒体にRFIDチップを付加したRFID搭載記録媒体を用いる情報提供システムにおいて、(1)暗号化された情報と復号鍵をサーバーより配信し、前記暗号化された情報と前記復号鍵は前記記録媒体に、前記復号鍵に対応したIDを前記RFIDチップに記録する手段、(2)前記RFID搭載記録媒体から暗号化された情報を読み取る際に、前記RFIDチップから前記IDを読み取り、前記記録媒体から読み出した復号鍵と比較し、前記IDに対応する復号化鍵である場合は前記暗号化された情報を復号化して利用し、前記IDに対応しない復号化鍵の場合は前記暗号化された情報を復

号化しない手段、を備えたことを特徴とするRFID搭載記録媒体利用の情報保護管理システムとする。

【００１５】請求項４に記載されたシステムは、前記配信がインターネットを用いるものであることを特徴とする請求項１乃至３記載のRFID搭載記録媒体利用の情報保護管理システムとする。

【００１６】請求項５に記載されたシステムは、前記配信が専用線を用いるものであることを特徴とする請求項１乃至３記載のRFID搭載記録媒体利用の情報保護管理システムとする。

【００１７】請求項６に記載されたシステムは、前記配信が無線を用いるものであることを特徴とする請求項１乃至３記載のRFID搭載記録媒体利用の情報保護管理システムとする。

【００１８】本発明では、RFIDチップを搭載した記録媒体（RFID搭載記録媒体）を用い、情報を暗号化して記録媒体に記録し、RFIDチップに復号化鍵を書き込む手段などを備えたシステムを構築する。本発明では基本的に情報提供者側が復号化鍵をユーザーに提供する。もちろん、情報製作者と復号化鍵を配信する鍵提供者が異なっていてもよい。重要な点は、末端のユーザーが直接復号化鍵を目にすることができないシステムにすることである。

【００１９】情報提供者は情報を暗号化してRFID搭載記録媒体に記録して提供する。一方、ユーザーはレコード店やビデオ店などの店頭からRFID搭載記録媒体を入手する。RFID搭載記録媒体には通常、暗号化された情報が記録されている。ユーザーは、入手したRFID搭載記録媒体のうち、利用したい情報に対する鍵を情報提供者に要求する。インターネットを用いる場合には、インターネットより鍵が配信され、オンライン状態で直接RFID搭載記録媒体のRFIDに書き込まれる。店頭で鍵を受ける場合には、ユーザーは鍵を書き込んでもらうRFID搭載記録媒体を店に持って行き、店員を通して無線（RFID入出力装置）でRFIDに鍵を書き込んでもらう。鍵は基本的には情報ごとに用意される。

【００２０】ユーザーが暗号化情報を利用するときは通常の記録媒体と同じ扱い方をすればよいが、RFID搭載記録媒体用プレイヤーはRFID入出力装置が内蔵されてるものでなければならない。なぜなら、鍵はRFIDに記録されているからである。このプレイヤーを本発明ではRFIDリーダー／ライター付きプレイヤー（RFID入出力装置付きプレイヤー）と呼ぶ。RFID入出力装置でRFIDより読み取った鍵を用い、プレイヤーは暗号化情報を記録媒体から読み取ると同時に、RFIDに記録されている鍵を用いてデコーダーで復号化し、暗号化情報を元の情報にして出力装置で出力する。

【００２１】本発明の情報保護管理システムでユーザーが用いる装置は次のようなハードウェア構成である。RFID搭載記録媒体のRFIDは、CPU、セキュリティ処理ソフトウェアを記録したROM、復号化鍵を記録する不揮発性メモリ、予備のメモリであるRAMおよびアンテナから構成される。一方、RFID入出力装置はRFIDとアンテナから構成される。またRFID入出力装置を含むプレイヤーにはデコーダー（暗号解読ソフトウェア内蔵ＩＣチップ）が搭載されていて、RFID搭載記録媒体から読み取った鍵を用いて、暗号化情報の暗号解読を行う。

【００２２】先に情報ごとに鍵が異なると述べたが、この情報を識別するために情報ごとにＩＤを付け、記録媒体とRFIDに記録する。記録媒体にヘッダーを設け、情報の記録位置（アドレス）とともにＩＤ（情報ＩＤ）を記録する。なお、媒体に対する識別子である媒体ＩＤもヘッダーに記録しておく。

【００２３】インターネットまたは無線で鍵をダウンロードする際、ユーザーはＩＤ（情報識別子、情報ＩＤ）と媒体ＩＤを提供者側に知らせることにより、ＩＤに対応する鍵とＩＤがダウンロードされ、RFIDに記録される。RFID搭載記録媒体から情報を読み取る際、記録媒体のＩＤとRFIDチップのＩＤが一致しない場合には、不正記録媒体として暗号化情報の復号化は行われない。

【００２４】

【発明の実施の形態】本発明の実施の形態を図を用いて具体的に説明する。図１は、発明のハードウェアから見たシステム構成図である。RFID記録媒体1は情報記録面130（記録媒体）、RFIDチップ110（RFID）およびアンテナ120から構成され、アンテナはRFIDに接続されている。アンテナの長さによって電波の届く距離が異なる。本発明の情報保護管理システムにおいては、プレイヤー2にRFID入出力装置210が内蔵されたものを使用するが、RFID入出力装置210はRFID搭載記録媒体1同様にRFIDチップ211とアンテナ212から構成されている。アンテナはRFIDに内蔵させていてもよいが、小型のチップのために、アンテナ120、212がないとの電波の届く距離（動作距離）はコンマ数ミリメーター程度で、プレイヤーをデザインするときの制約となるおそれがある。そこで、本発明の形態では記録媒体130に影響のないように円形のアンテナを外付けの形で取り付けてある。本発明の形態では、電波の届く範囲（動作距離）を２～３センチメーターに延ばすことができる。また本発明で使用するRFID110、211の仕様の一例を以下に挙げる。

RF　：ISO14443-B
CPU　：8bits
不揮発性メモリ　：32Kbits
ROM　：23Kbits
RAM　：1Kbits

【００２５】RFは“Radio Frequency”の略で、電波周波数の規格はISO14443-Bとしている。不揮発性メモリとRAMは基本的に違いはないが、前者には鍵を保存し、後者は予備（例えば、ＩＤの保存）として使用する。いずれもリード・ライト可能なメモリであるが、通常のRAM

と異なり、不揮発性のメモリである。上記のRAM、不揮発性メモリのメモリサイズは一例であり、鍵の長さやＩＤの長さ、あるいはその個数によって使用するメモリサイズは異なる。ROMにはセキュリティ処理用ソフトウェアが記録されていて、不正アクセスを防止する。

【００２６】プレイヤー2には記録媒体から暗号化情報を読み取るためのヘッド（ＣＤやＤＶＤの場合には光学式読み取り式ヘッド）が付いているが、図では省略してある。記録媒体130から読み取った暗号化情報は、RFID入力装置（RFID211）で読み取った鍵で復号化を行うが、この復号化を行っているのがデコーダー230（暗号解読ソフトウェア内蔵のＩＣチップ）である。

【００２７】図の例では、プレイヤー2で復号化した情報の出力先をパソコン3（ＰＣ）としている。すなわちユーザーが目にする（あるいは耳にする）結果は、パソコンに接続のディスプレイやスピーカー（図示省略）に出力された映像や音である。

【００２８】なお、本発明では記録媒体に情報の書き込み（追記）を行う形態も可能である。その場合にはプレイヤーには記録媒体に対するリード機能だけでなく、ライト機能も必要である（例えば、CD-RやDVD-Rなど）。またRFID搭載の磁気記録媒体とRFID入力装置内蔵のハードディスクを用いれば、ハードディスクに対しても本発明の情報保護管理システムが利用できる。取り外し型のハードディスクも可能あるが、本発明の主旨にあった大容量記録媒体としては光磁気記録媒体（ＭＯ、ＭＤ）が好ましい。

【００２９】ユーザーが暗号化情報を復号化するための鍵をインターネット9より受け取るには、まず　ＰＣ3で鍵提供者のサイトに接続し、媒体ＩＤと情報ＩＤを情報提供者側に知らせる。情報提供者側はその情報に基づき、対応する鍵をインターネットで配信し、ユーザー側はＰＣを介して直接鍵をプレイヤー2のRFID211に送信する。RFID211は入力情報（この場合は鍵）に対してセキュリティ処理を行い、セキュリティ上問題ないときにはRFID110に送信する。RFID110は入力情報に対してセキュリティ処理を行い、問題がない場合はRFID110の不揮発性メモリに鍵を書き込む。これにより、ユーザーは鍵に対応する情報が利用できるようになる。

【００３０】記録媒体に書き込み可能なプレイヤー2を使用する場合には、ユーザーは情報を直接受けることができ、情報提供者から送られてくる暗号化情報と鍵に対し、鍵はRFID110に書き込み、暗号化情報は記録媒体130に書き込む。鍵と暗号化情報を分割して記録し、しかも鍵をRFID110に記録するために、記録媒体130に記録された暗号化情報がコピーされても、RFID110の鍵はコピーされることはないから、コピーによる情報の不正利用はできない。鍵や情報の書き込みは本発明の情報保護管理システムが自動的に行うために、鍵がユーザーに知られることはない。

【００３１】図２は、RFID搭載記録媒体のデータ構造の一例である。記録媒体130にはヘッダーHと暗号化情報（データ）とから構成される。商品番号と媒体ＩＤでこの媒体を特定できる。個別情報記録欄に情報の識別子であるＩＤｎと暗号化情報の記録位置であるアドレスＰｎが登録されていて、暗号化情報ＣｎをＰｎで直接ポイントしている（図ではｎは数値）。暗号化情報Ｃｎはヘッダー Ｈｎ付きで暗号化されている。ユーザーが望む情報に対する鍵を入手する場合、鍵提供者に知らせる情報は商品番号（場合によっては媒体ＩＤ）と情報ＩＤ（ＩＤ１、ＩＤ２等）である。一方、RFID110の不揮発性メモリに鍵Ｋｎを記録し、RAMにＩＤｎを記録する。ＫｎとＩＤｎは１対１の関係にある。

【００３２】ＩＤｎとＫｎを同時に受信する形態では、ＩＤｎは記録媒体130とRFID110に書き込む。暗号化情報を読み取るときには、復号化の前にまず前記の両ＩＤｎを比較し、一致する場合にのみ復号化を行う。すなわち、ＩＤｎは単に情報を識別するだけでなく、情報保護の働きも持っている。

【００３３】本発明では鍵だけでなく、情報も同時に配信することができる。例えば図の例では、ユーザーが提供者側から暗号化情報Ｃｊ、鍵Ｋｊ、情報識別子ＩＤｊを同時に受信し、プレイヤーがそれぞれの情報（データ）を①、②、③、④の順序でそれぞれの保存場所に記録する。このとき情報保護管理システムは、すでに情報が記録されている場所に重複して情報が書き出されないようにチェックする。なお情報識別子ＩＤｊや暗号化情報Ｃｊを記録媒体130に書き出す形態においては、プレイヤーにリード・ライト機能が備わっていることが必要である（例えば、CD-Rなど）。

【００３４】

【実施例】図３は、本発明における情報（音楽、映像、ゲームソフトなど）とRFID搭載記録媒体の流れを示した一例である。ユーザー5は店6（レコード店やビデオ店など）で暗号化された情報を含むRFID搭載記録媒体1を購入650し、自宅のプレイヤー52で実行し、記録媒体の情報を楽しむことができる。RFID搭載記録媒体1の情報は暗号化されているために、鍵のない情報は利用することができない。そこで、インターネット9に接続している場合には、インターネットで鍵提供者7のサーバーS7に接続し、商品番号、媒体ＩＤ、情報ＩＤを送信570し、購入したい情報に対応した鍵を要求する。要求を受けた鍵提供者7は鍵を配信750する。鍵はプレイヤー52によってRFIDに書き込まれる。

【００３５】一方、インターネット9に接続できないユーザー5の場合には、インターネットから鍵の提供を受けられないため、利用した情報がある場合には、RFID搭載記録媒体1を店6に持ち込み561、店のプレイヤー62で鍵をRFIDに書き込んでもらう。この例では、鍵は店が管理しているのではなく、鍵提供者7から配信してもらう

形態にしている。すなわち、店はインターネットを通じて鍵提供者のサーバーS7に接続し、ユーザーの望む情報に対する商品番号、媒体ＩＤ、情報ＩＤなどを送信670する。サーバーS7は要請のあった情報に対する鍵を配信760する。鍵を受けたプレイヤー62はRFID搭載記録媒体1のRFIDに鍵を書き込む。ユーザーは鍵の書き込まれたRFID搭載記録媒体1を家に持ち帰り651、家のプレイヤー52で鍵の記録されている情報を再生して楽しむことができる。

【００３６】同様の手順で鍵だけでなく、情報の提供も店やインターネットを通じて受けることができる。ただし、ユーザーが自宅でインターネットを通じて情報を受ける場合には、プレイヤー52はRFID搭載記録媒体の記録媒体に情報が書き込める機能を有している必要がある。なお課金については本発明の範疇でないから、ここでは省略する。

【００３７】

【発明の効果】本発明はRFID記録媒体を用いることによって、コピーによる情報の不正使用を防止し、情報の保護管理を可能にしたシステムである。情報は暗号化されて記録媒体に記録され、鍵（暗号解読鍵）あるいはＩＤコードは、RFIDチップに記録されているために、記録媒体の暗号化情報をコピーできても、鍵はコピーできない。従って、コピーされた暗号化情報が不正に利用されることはない。

【００３８】記録媒体の大容量化が進むなか、１枚の記録媒体に多数の情報（例えば音楽の場合には数十曲）が同時に記録できる。しかし、ユーザーにしてみれば、必ずしもすべてが欲しいわけではない。これに対して、本発明では欲しい情報のみを選択して鍵を購入する形態で情報を提供している。もちろん、初期時は記録媒体も購入しなければならないが、安く手に入る。さらに情報を追加して利用したい場合には、インターネットで鍵のみを購入すればよいから手順が楽である。しかも記録媒体の購入が不要であるために、単体の記録媒体で情報を購入するよりもはるかに安価で入手可能となる。

【００３９】一方、情報提供者側にしてみれば、複数の情報を同時にコピーした記録媒体をユーザーに提供する形態がとれるために、効率のよい商品製作が可能となる。またユーザーに提供する情報の組み合わせによってユーザーニーズを刺激する商品を企画・製作できる。しかも、初めは購入したくない情報も同一の記録媒体に存在することによって、ユーザーが新たに追加注文してくる機会が増加することも期待できる。その場合にも、媒体はすでにユーザーの手元にあるから、鍵のみの販売でよく、商品流通の簡素化が可能であり、効率的な販売戦略が立てられる。追記型あるいは全面書き込み型の販売も可能であり、効率的かつ効果的な商品販売が実現できる。

【００４０】このような情報の販売方法が可能なのも、本発明の情報保護管理システムによって、情報がコピーによる不正使用されることに対して完全防備されているからである。

【図面の簡単な説明】

【図１】本発明のRFID搭載記録媒体利用のダウンロード型情報保護管理システムのブロック図である。

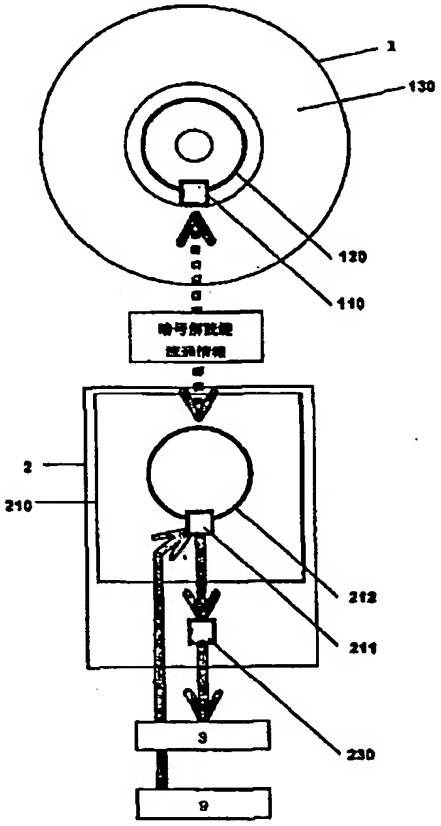
【図２】本発明の情報保護管理システムで用いるRFID搭載記録媒体のデータ構造の一例を説明するための図である。

【図３】本発明の情報保護管理システムにおけるRFID搭載記録媒体と情報の流れを説明するための図である。

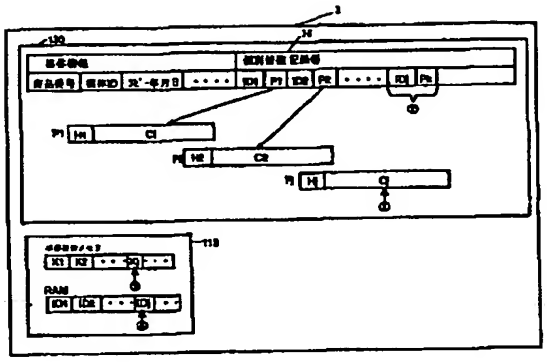
【符号の説明】

1	RFID搭載記録媒体（RFID搭載記録媒体：CD、DVDなど）
１１０	RFIDチップ
１２０	アンテナ（タグ）
１３０	記録媒体面（記録媒体）
2	RFIDリーダー／ライター付きプレイヤー（RFID入出力装置付きプレイヤー）
２１０	RFIDリーダー／ライター（RFID入出力装置）
２１１	RFIDチップ
２１２	アンテナ（タグ）
２３０	デコーダー（ハードウェア化された暗号解読ソフトウェア）
3	パソコン（ＰＣ）
5	ユーザー（顧客）
５２	RFID入出力装置付きプレイヤー
５６１	持ち込み
５７０	送信
ＰＣ５	パソコン
6	店（レコード店、ビデオ店など）
６２	RFID入出力装置付きプレイヤー
６５０	購入
６５１	持ち帰り
６７０	送信
ＰＣ６	パソコン
7	鍵提供者
７５０	配信
７６０	配信
Ｓ７	サーバー
9	インターネット
H、Hn	ヘッダー
Ｐn	ポインタ（暗号化情報が記録されている先頭のアドレス）
ＩＤn	情報識別子（情報ＩＤ）
Ｋn	鍵（復号化鍵、暗号解読鍵）
媒体ＩＤ	媒体識別子

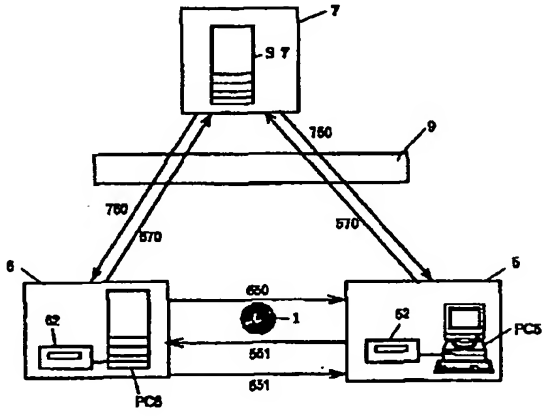
【図１】


1
130
120
110
2
210
212
211
3
230
9

【図２】



【図３】


7
9 7
760
9
760
570
570
6
5
650
1
62
62
PC5
651
651
PC6

フロントページの続き

Ｆターム(参考) 5B035 AA13 BB09 BC05 CA23
5J104 AA13 AA16 EA16 NA02 NA27
NA37 PA07